3 of whom shall not be employees of any Federal Government agency or Federal Government contractor.

(B) No individual may be appointed to the Committee under subparagraph (A) unless the Secretary and the Directly jointly determine that the individual—

(i) qualifies for a security clearance at the secret level or higher;

(ii) possesses scientific, medical, or technical expertise pertinent to some aspect of the investigation and analysis of unidentified aerial phenomena; and

(iii) has previously conducted research or writing that demonstrates scientific, technological, or operational knowledge regarding aspects of the subject matter, including propulsion, aerodynamic control, signatures, structures, materials, sensors, countermeasures, weapons, electronics, power generation, field investigations, forensic examination of particular cases, analysis of open source and classified information regarding domestic and foreign research and commentary, and historical information pertaining to unidentified aerial phenomena.

(C) The Secretary and Director may terminate the membership of any individual on the Committee upon a finding by the Secretary and the Director jointly that the member no longer meets the criteria specified in this subsection.

(3) CHAIRPERSON.—The Secretary shall, in coordination with the Director, designate a temporary Chairperson of the Committee, but at the earliest practicable date the Committee shall elect a Chairperson from among its members, who will serve a term of 2 years, and is eligible for re-election.

(4) EXPERT ASSISTANCE, ADVICE, AND RECOMMENDATIONS.—(A) The Committee may, upon invitation of the head of the Office, provide expert assistance or advice to any line organization designated to carry out field investigations or data analysis as authorized by subsections (d) and (e).

(B) The Committee, on its own initiative, or at the request of the Director, the Secretary, or the head of the Office, may provide advice and recommendations regarding best practices with respect to the gathering and analysis of data on unidentified aerial phenomena in general, or commentary regarding specific incidents, cases, or classes of unidentified aerial phenomena.

(5) REPORT.—Not later than December 31, 2022, and not later than December 31 of each year thereafter, the Committee shall submit a report summarizing its activities and recommendations to the following:

(A) The Secretary.

(B) The Director.

(C) The head of the Office.

(D) The Committee on Armed Services, the Select Committee on Intelligence, and the Committee on Appropriations of the Senate.

(E) The Committee on Armed Services, the Permanent Select Committee on Intelligence, and the Committee on Appropriations of the House of Representatives.

(6) RELATION TO FACA.—For purposes of the Federal Advisory Committee Act (5 U.S.C. App.), the Committee shall be considered an advisory committee (as defined in section 3 of such Act, except as otherwise provided in the section or as jointly deemed warranted by the Secretary and the Director under section 4(b)(3) of such Act.

(7) TERMINATION OF COMMITTEE.—The Committee shall terminate on the date that is six years after the date of the establishment of the Committee.

(m) DEFINITIONS.—In this section:

(1) The term ''appropriate committees of Congress'' means—

(A) the Committee on Armed Services, the Select Committee on Intelligence, the Committee on Foreign Relations, and the Committee on Appropriations of the Senate; and

(B) the Committee on Armed Services, the Permanent Select Committee on Intelligence, the Committee on Foreign Affairs, and the Committee on Appropriations of the House of Representatives.

(2) The term ''intelligence community'' has the meaning given such term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(3) The term ''transmedium objects or devices'' means objects or devices that are observed to transition between space and the atmosphere, or between the atmosphere and bodies of water, that are not immediately identifiable.

(4) The term ''unidentified aerial phenomena'' means—

(A) airborne objects that are not immediately identifiable;

(B) transmedium objects or devices; and

(C) submerged objects or devices that are not immediately identifiable and that display behavior or performance characteristics suggesting that they may be related to the subjects described in subparagraph (A) or (B).

SA 4811. Mr. TUBERVILLE (for himself and Mr. BRAUN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. PROHIBITING THE INTERNAL REVENUE SERVICE FROM REQUIRING FINANCIAL INSTITUTIONS TO REPORT ON FINANCIAL TRANSACTIONS OF CUSTOMERS.

(a) IN GENERAL.—Subject to subsection (b), the Internal Revenue Service shall not be permitted to create or implement any new financial account information reporting program that—

(1) was not in effect as of October 1, 2021, and

(2) would require financial institutions to report data on financial accounts in an information return listing balances, transactions, transfers, or inflows or outflows of any kind.

(b) RULE OF CONSTRUCTION.—

(1) IN GENERAL.—Nothing in this section shall preempt, limit, or supersede, or be construed to preempt, limit, or supersede, any provision of, or requirement under, the Bank Secrecy Act or any regulations promulgated under such Act.

(2) DEFINITION.—For purposes of this subsection, the term ''Bank Secrecy Act'' means—

(A) section 21 of the Federal Deposit Insurance Act (12 U.S.C. 1829b),

(B) chapter 2 of title I of Public Law 91–508 (12 U.S.C. 1951 et seq.), and

(C) subchapter II of chapter 53 of title 31, United States Code.

SA 4812. Mr. TUBERVILLE submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. PROHIBITING TSP INVESTMENT IN CHINA.

(a) FINDINGS.—Congress finds the following:

(1) The Thrift Savings Fund invests more than $700,000,000,000 on behalf of plan participants. As the guardian of the retirement funds of approximately 6,000,000 Federal civilian and military plan participants, it is critical that sums in the Thrift Savings Fund are not invested in securities linked to the economy of the People's Republic of China.

(2) Companies headquartered in the People's Republic of China have repeatedly committed corporate espionage, violated sanctions imposed by the United States, flouted international property laws, committed theft, and failed to comply with audit and regulatory standards designed to safeguard investors.

(3) The Thrift Savings Plan is known for its low management fees and comprehensive array of investment strategies. The provisions of this section, and the amendments made by this section, will not increase fees imposed on participants of the Thrift Savings Plan.

(4) The November 2017 selection of the MSCI ACWI Index by the Federal Retirement Thrift Investment Board, initially scheduled to be effective in 2020, would violate the terms of subsection (i) of section 8438 of title 5, United States Code, as added by subsection (b)(1) of this section.

(b) PROHIBITION ON ANY TSP FUND INVESTING IN ENTITIES BASED IN THE PEOPLE'S REPUBLIC OF CHINA.—

(1) IN GENERAL.—Section 8438 of title 5, United States Code, is amended by adding at the end the following:

''(i) Notwithstanding any other provision of this section, no fund established or overseen by the Board may include an investment in any security of—

''(1) an entity based in the People's Republic of China; or

''(2) any subsidiary that is owned or operated by an entity described in paragraph (1).''.

(2) DIVESTITURE OF ASSETS.—Not later than 30 days after the date of enactment of this Act, the Federal Retirement Thrift Investment Board established under section 8472(a) of title 5, United States Code, shall—

(A) review whether any sums in the Thrift Savings Fund are invested in violation of subsection (i) of section 8438 of that title, as added by paragraph (1) of this subsection;

(B) if any sums are invested in the manner described in subparagraph (A), divest those sums in a manner that is consistent with the legal and fiduciary duties provided under chapter 84 of that title, or any other applicable provision of law; and

(C) reinvest any sums divested under subparagraph (B) in investments that do not violate subsection (i) of section 8438 of that title, as added by paragraph (1) of this subsection.

(c) PROHIBITION ON INVESTMENT OF TSP FUNDS IN ENTITIES BASED IN THE PEOPLE'S REPUBLIC OF CHINA THROUGH THE TSP MUTUAL FUND WINDOW.—Section 8438(b)(5) of title 5, United States Code, is amended by adding at the end the following:

''(E) A mutual fund accessible through a mutual fund window authorized under this

paragraph may not include an investment in any security of—

''(i) an entity based in the People's Republic of China; or

''(ii) any subsidiary that is owned or operated by an entity described in clause (i).''.

SA 4813. Mr. SCOTT of Florida submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

DIVISION E—CYBER INCIDENT REPORTING ACT OF 2021 AND CISA TECHNICAL CORRECTIONS AND IMPROVEMENTS ACT OF 2021

TITLE LI—CYBER INCIDENT REPORTING ACT OF 2021

SEC. 5101. SHORT TITLE.

This title may be cited as the ''Cyber Incident Reporting Act of 2021''.

SEC. 5102. DEFINITIONS.

In this title:

(1) COVERED CYBER INCIDENT; COVERED ENTITY; CYBER INCIDENT.—The terms ''covered cyber incident'', ''covered entity'', and ''cyber incident'' have the meanings given those terms in section 2230 of the Homeland Security Act of 2002, as added by section 5103 of this title.

(2) DIRECTOR.—The term ''Director'' means the Director of the Cybersecurity and Infrastructure Security Agency.

(3) INFORMATION SYSTEM; RANSOM PAYMENT; RANSOMWARE ATTACK; SECURITY VULNERABILITY.—The terms ''information system'', ''ransom payment'', ''ransomware attack'', and ''security vulnerability'' have the meanings given those terms in section 2200 of the Homeland Security Act of 2002, as added by section 5203 of this division.

SEC. 5103. CYBER INCIDENT REPORTING.

(a) CYBER INCIDENT REPORTING.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(1) in section 2209(b) (6 U.S.C. 659(b)), as so redesignated by section 5203(b) of this division—

(A) in paragraph (11), by striking ''and'' at the end;

(B) in paragraph (12), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(13) receiving, aggregating, and analyzing reports related to covered cyber incidents (as defined in section 2230) submitted by covered entities (as defined in section 2230) and reports related to ransom payments submitted by entities in furtherance of the activities specified in sections 2202(e), 2203, and 2231, this subsection, and any other authorized activity of the Director, to enhance the situational awareness of cybersecurity threats across critical infrastructure sectors.''; and

(2) by adding at the end the following:

''Subtitle C—Cyber Incident Reporting

''SEC. 2230. DEFINITIONS.

''In this subtitle:

''(1) CENTER.—The term 'Center' means the center established under section 2209.

''(2) COUNCIL.—The term 'Council' means the Cyber Incident Reporting Council described in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)).

''(3) COVERED CYBER INCIDENT.—The term 'covered cyber incident' means a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the final rule issued pursuant to section 2232(b).

''(4) COVERED ENTITY.—The term 'covered entity' means—

''(A) any Federal contractor; or

''(B) an entity that owns or operates critical infrastructure that satisfies the definition established by the Director in the final rule issued pursuant to section 2232(b).

''(5) CYBER INCIDENT.—The term 'cyber incident' has the meaning given the term 'incident' in section 2200.

''(6) CYBER THREAT.—The term 'cyber threat'—

''(A) has the meaning given the term 'cybersecurity threat' in section 2200; and

''(B) does not include any activity related to good faith security research, including participation in a bug-bounty program or a vulnerability disclosure program.

''(7) FEDERAL CONTRACTOR.—The term 'Federal contractor' means a business, nonprofit organization, or other private sector entity that holds a Federal Government contract or subcontract at any tier, grant, cooperative agreement, or other transaction agreement, unless that entity is a party only to—

''(A) a service contract to provide housekeeping or custodial services; or

''(B) a contract to provide products or services unrelated to information technology that is below the micro-purchase threshold, as defined in section 2.101 of title 48, Code of Federal Regulations, or any successor regulation.

''(8) FEDERAL ENTITY; INFORMATION SYSTEM; SECURITY CONTROL.—The terms 'Federal entity', 'information system', and 'security control' have the meanings given those terms in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

''(9) SIGNIFICANT CYBER INCIDENT.—The term 'significant cyber incident' means a cybersecurity incident, or a group of related cybersecurity incidents, that the Secretary determines is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States.

''(10) SMALL ORGANIZATION.—The term 'small organization'—

''(A) means—

''(i) a small business concern, as defined in section 3 of the Small Business Act (15 U.S.C. 632); or

''(ii) any nonprofit organization, including faith-based organizations and houses of worship, or other private sector entity with fewer than 200 employees (determined on a full-time equivalent basis); and

''(B) does not include—

''(i) a business, nonprofit organization, or other private sector entity that is a covered entity; or

''(ii) a Federal contractor.

''SEC. 2231. CYBER INCIDENT REVIEW.

''(a) ACTIVITIES.—The Center shall—

''(1) receive, aggregate, analyze, and secure, using processes consistent with the processes developed pursuant to the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.) reports from covered entities related to a covered cyber incident to assess the effectiveness of security controls, identify tactics, techniques, and procedures adversaries use to overcome those controls and other cybersecurity purposes, including to support law enforcement investigations, to assess potential impact of incidents on public health and safety, and to have a more accurate picture of the cyber threat to critical infrastructure and the people of the United States;

''(2) receive, aggregate, analyze, and secure reports to lead the identification of tactics, techniques, and procedures used to perpetuate cyber incidents and ransomware attacks;

''(3) coordinate and share information with appropriate Federal departments and agencies to identify and track ransom payments, including those utilizing virtual currencies;

''(4) leverage information gathered about cybersecurity incidents to—

''(A) enhance the quality and effectiveness of information sharing and coordination efforts with appropriate entities, including agencies, sector coordinating councils, information sharing and analysis organizations, technology providers, critical infrastructure owners and operators, cybersecurity and incident response firms, and security researchers; and

''(B) provide appropriate entities, including agencies, sector coordinating councils, information sharing and analysis organizations, technology providers, cybersecurity and incident response firms, and security researchers, with timely, actionable, and anonymized reports of cyber incident campaigns and trends, including, to the maximum extent practicable, related contextual information, cyber threat indicators, and defensive measures, pursuant to section 2235;

''(5) establish mechanisms to receive feedback from stakeholders on how the Agency can most effectively receive covered cyber incident reports, ransom payment reports, and other voluntarily provided information;

''(6) facilitate the timely sharing, on a voluntary basis, between relevant critical infrastructure owners and operators of information relating to covered cyber incidents and ransom payments, particularly with respect to ongoing cyber threats or security vulnerabilities and identify and disseminate ways to prevent or mitigate similar incidents in the future;

''(7) for a covered cyber incident, including a ransomware attack, that also satisfies the definition of a significant cyber incident, or is part of a group of related cyber incidents that together satisfy such definition, conduct a review of the details surrounding the covered cyber incident or group of those incidents and identify and disseminate ways to prevent or mitigate similar incidents in the future;

''(8) with respect to covered cyber incident reports under section 2232(a) and 2233 involving an ongoing cyber threat or security vulnerability, immediately review those reports for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to appropriate stakeholders, in coordination with other divisions within the Agency, as appropriate;

''(9) publish quarterly unclassified, public reports that may be based on the unclassified information contained in the briefings required under subsection (c);

''(10) proactively identify opportunities and perform analyses, consistent with the protections in section 2235, to leverage and utilize data on ransomware attacks to support law enforcement operations to identify, track, and seize ransom payments utilizing virtual currencies, to the greatest extent practicable;

''(11) proactively identify opportunities, consistent with the protections in section 2235, to leverage and utilize data on cyber incidents in a manner that enables and strengthens cybersecurity research carried out by academic institutions and other private sector organizations, to the greatest extent practicable;